AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A random sequence generating apparatus for generating a sequence of integers of w bits, comprising:

a seed receiving section which receives a sequence of integers $s_1, s_2, ..., s_n, ..., s_m$ of w bits as a seed for integers n and m ($1 \leq n \leq m-1$);

an initialization section which provides a transformation section with said received sequence of integers $s_1, s_2, ..., s_n, ..., s_m$ as an integer sequence $x_1, x_2, ..., x_n, ..., x_m$;

said transformation section which performs predetermined transformation on each of said provided integer sequence $x_1, x_2, ..., x_n, ..., x_m$ to acquire a sequence of integers $y_1, y_2, ..., y_n, ..., y_m$ of w bits;

a rotation section which acquires a number of rotation bits from said sequence of integers $y_{n+1}, ..., y_m$, performs a rotation operation on said acquired number of rotation bits with respect to all of or a part of said sequence of integers $y_1, y_2, ..., y_n, ..., y_m$ taken as a bit sequence of wm bits, and acquires a sequence of integers $z_1, z_2, ..., z_n, ..., z_m$ of w bits from said acquired bit sequence of wm bits;

an updating section which provides said transformation section with said sequence of integers $z_1, z_2, ..., z_n, ..., z_m$ as said integer sequence $x_1, x_2, ..., x_n, ..., x_m$; and

an output section which outputs a sequence of integers $z_1, z_2, ..., z_n$ or $z_{n+1}, ..., z_m$ obtained last as a random sequence $r_1, r_2, ..., r_n$ or $r_1, ..., r_{m-n}$ respectively in case where transformation in said transformation section and rotation in said rotation section are repeated a predetermined number of times,

a mapping $g(\cdot,\cdot)$ defined as

$$g(a, b) = 2b^2 + h(a)b + q(\text{mod } 2^w)$$

with h(·) being a predetermined mapping and q being a predetermined integer ($0 \leq q \leq 2^{w-1}$), the mapping h(·) being defined by an operation of setting 01 to least significant two bits in a numerical expression of a given value,

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i ($1 \leq i \leq m-1$):

$$y_1 = g(x_m, x_1),$$

$$y_{i+1} = g(x_i, x_{i+1}),$$

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i ($1 \leq i \leq m-1$) and a predetermined integer c:

$$y_1 = g(c, x_1),$$

$$y_{i+1} = g(y_i, x_{i+1}),$$

or

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i ($1 \leq i \leq m-1$) and a predetermined integer c:

$$y_1 = g(c, x_1),$$

$$y_{i+1} = g(x_i, x_{i+1}).$$

2. – 7. (Cancelled)

8. (Currently Amended) The random sequence generating apparatus according to claim [[5]] 1, wherein said mapping h(·) is defined by an operation of inverting a predetermined bit in a numerical expression of a given value instead of the operation of setting 01 to the least significant two bits.

9. (Cancelled)

10. (Previously Presented) The random sequence generating apparatus according to claim 1, wherein taking said sequence of integers y_{n+1}, ..., y_m as a bit sequence of w(m-n) bits, said rotation section acquires, as said number of rotation bits, an integer value equivalent to a bit

sequence taken as an integer and obtained by arranging at least one bit at a predetermined position extracted from said bit sequence.

11. (Previously Presented) The random sequence generating apparatus according to claim 10, wherein taking said sequence of integers y_{n+1}, ..., y_m as a bit sequence of w(m-n) bits, said rotation section determines a direction of rotation based on a value of a bit at a predetermined position in said bit sequence.

12. (Previously Presented) The random sequence generating apparatus according to claim 1, wherein said rotation section acquires a number of rotation bits from said sequence of integers y_{n+1}, ..., y_m, performs a rotation operation on said acquired number of rotation bits with respect to said sequence of integers y_1, y_2, ..., y_n, ..., y_m taken as a bit sequence of wn bits, acquires a sequence of integers z_1, z_2, ..., z_n of w bits from said acquired bit sequence of wn bits, performs a rotation operation on said acquired number of rotation bits with respect to said sequence of integers y_{n+1}, ..., y_m taken as a bit sequence of w(m-n) bits, and acquires a sequence of integers z_{n+1}, ..., z_m of w bits from said acquired bit sequence of w(m-n) bits.

13. (Currently Amended) An encryption/decryption apparatus comprising:

a random sequence generating section which generates a random sequence r_1, r_2, ..., r_n by ~~means of~~ a random sequence generating apparatus recited in claim 1;

a message receiving section which receives a sequence of integers p_1, p_2, ..., p_i, ... of w bits as a message; and

an encryption/decryption section which outputs a sequence of integers p_1 xor r_1, p_2 xor r_2, ..., p_i xor $r_{((i+n-1) \bmod n)+1}$, ...as a result of encryption or decryption.

14. (Currently Amended) A random sequence generating method executed by a random sequence generating apparatus having a seed receiving section, an initializing section, a transformation section, a rotation section, an updating section, and an output section for generating a sequence of integers of w bits, said random sequence generating method comprising:

a seed receiving step in which said receiving section receives a sequence of integers s_1, s_2, ..., s_n, ..., s_m of w bits as a seed for integers n and m ($1 \leq n \leq m-1$);

an initialization step in which said initializing section provides a transformation step with said received sequence of integers s_1, s_2, ..., s_n, ..., s_m as an integer sequence x_1, x_2, ..., x_n, ..., x_m;

said transformation step in which said transformation section performs predetermined transformation on each of said provided integer sequence x_1, x_2, ..., x_n, ..., x_m to acquire a sequence of integers y_1, y_2, ..., y_n, ..., y_m of w bits;

a rotation step in which said rotation section acquires a number of rotation bits from said sequence of integers y_{n+1}, ..., y_m, performs a rotation operation on said acquired number of rotation bits with respect to all of or a part of said sequence of integers y_1, y_2, ..., y_n, ..., y_m taken as a bit sequence of wm bits, and acquires a sequence of integers z_1, z_2, ..., z_n, ..., z_m of w bits from said acquired bit sequence of wm bits;

an updating step in which said updating section provides said transformation step with said sequence of integers z_1, z_2, ..., z_n, ..., z_m as said integer sequence x_1, x_2, ..., x_n, ..., x_m; and

an output step in which said output section outputs a sequence of integers z_1, z_2, ..., z_n or z_{n+1}, ..., z_m obtained last as a random sequence r_1, r_2, ..., r_n or r_1, ..., r_{m-n} respectively in case where transformation in said transformation step and rotation in said rotation step are repeated a predetermined number of times,

a mapping $g(\cdot,\cdot)$ defined as

$$g(a, b) = 2b^2 + h(a)b + q(\mathrm{mod}\ 2^w)$$

with $h(\cdot)$ being a predetermined mapping and q being a predetermined integer ($0 \leq q \leq 2^{w-1}$), the mapping $h(\cdot)$ being defined by an operation of setting 01 to least significant two bits in a numerical expression of a given value,

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i ($1 \leq i \leq m-1$):

$$y_1 = g(x_m, x_1),$$

$$y_{i+1} = g(x_i, x_{i+1}),$$

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i ($1 \leq i \leq m-1$) and a predetermined integer c:

$$y_1 = g(c, x_1),$$

$$y_{i+1} = g(y_i, x_{i+1}),$$

or

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i ($1 \leq i \leq m-1$) and a predetermined integer c:

$$y_1 = g(c, x_1),$$

$$y_{i+1} = g(x_i, x_{i+1}).$$

15. – 20. (Cancelled)

21. (Currently Amended) The random sequence generating method according to claim [[18]] 14, wherein said mapping $h(\cdot)$ is defined by an operation of inverting a predetermined bit in a numerical expression of a given value instead of the operation of setting 01 to the least significant two bits.

22. (Cancelled)

23. (Previously Presented) The random sequence generating method according to claim 14, wherein taking said sequence of integers y_{n+1}, ..., y_m as a bit sequence of w(m-n) bits, said rotation step acquires, as said number of rotation bits, an integer value equivalent to a bit sequence taken as an integer and obtained by arranging at least one bit at a predetermined position extracted from said bit sequence.

24. (Previously Presented) The random sequence generating method according to claim 23, wherein taking said sequence of integers y_{n+1}, ..., y_m as a bit sequence of w(m-n) bits, said rotation step determines a direction of rotation based on a value of a bit at a predetermined position in said bit sequence.

25. (Previously Presented) The random sequence generating method according to claim 14, wherein said rotation step acquires a number of rotation bits from said sequence of integers y_{n+1}, ..., y_m, performs a rotation operation on said acquired number of rotation bits with

respect to said sequence of integers y_1, y_2, ..., y_n, ..., y_m taken as a bit sequence of wn bits, acquires a sequence of integers z_1, z_2, ..., z_n of w bits from said acquired bit sequence of wn bits, performs a rotation operation on said acquired number of rotation bits with respect to said sequence of integers y_{n+1}, ..., y_m taken as a bit sequence of w(m-n) bits, and acquires a sequence of integers z_{n+1}, ..., z_m of w bits from said acquired bit sequence of w(m-n) bits.

26. (Currently Amended) An encryption/decryption method executed by an encryption/decryption apparatus having a random sequence generating section, a message receiving section, and an encryption/decryption section, said encryption/decryption method comprising:

a random sequence generating step in which said random sequence generating section generates a random sequence r_1, r_2, ..., r_n by ~~means of~~ a random sequence generating method recited in claim 14;

a message receiving step in which said message receiving section receives a sequence of integers p_1, p_2, ..., p_i, ... of w bits as a message; and

an encryption/decryption step in which said encryption/decryption section outputs a sequence of integers p_1 xor r_1, p_2 xor r_2, ..., p_i xor $r_{((i+n-1) \bmod n)+1}$, ... as a result of encryption or decryption.

27. (Currently Amended) A computer readable medium recording a program ~~product~~ which allows a computer to function as:

a seed receiving section which receives a sequence of integers s_1, s_2, ..., s_n, ..., s_m of w bits as a seed for integers n and m ($1 \leq n \leq m-1$);

an initialization section which provides a transformation section with said received sequence of integers s_1, s_2, ..., s_n, ..., s_m as an integer sequence x_1, x_2, ..., x_n, ..., x_m;

a transformation section which performs predetermined transformation on each of said provided integer sequence to acquire a sequence x_1, x_2, ..., x_n, ..., x_m to acquire a sequence of integers y_1, y_2, ..., y_n, ... y_m of w bits;

a rotation section which acquires a number of rotation bits from said sequence of integers y_{n+1}, ..., y_m, performs a rotation operation on said acquired number of rotation bits with respect

to all of or a part of said sequence of integers $y_1, y_2, \ldots, y_n, \ldots, y_m$ taken as a bit sequence of wm bits, and acquires a sequence of integers $z_1, z_2, \ldots, z_n, \ldots, z_m$ of w bits from said acquired bit sequence of wm bits;

an updating section which provides said transformation section with said sequence of integers $z_1, z_2, \ldots, z_n, \ldots, z_m$ as said integer sequence $x_1, x_2, \ldots, x_n, \ldots, x_m$; and

an output section which outputs a sequence of integers $z_1, z_2, \ldots, z_n$ or $z_{n+1}, \ldots, z_m$ obtained last as a random sequence $r_1, r_2, \ldots, r_n$ or $r_1, \ldots, r_{m-n}$ respectively in case where transformation in said transformation section and rotation in said rotation section are repeated a predetermined number of times,

a mapping $g(\cdot,\cdot)$ defined as

$$g(a, b) = 2b^2 + h(a)b + q(\mathrm{mod}\ 2^w)$$

with $h(\cdot)$ being a predetermined mapping and q being a predetermined integer $(0 \le q \le 2^{w-1})$, the mapping $h(\cdot)$ being defined by an operation of setting 01 to least significant two bits in a numerical expression of a given value,

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i $(1 \le i \le m-1)$:

$$y_1 = g(x_m, x_1),$$

$$y_{i+1} = g(x_i, x_{i+1}),$$

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i $(1 \le i \le m-1)$ and a predetermined integer c:

$$y_1 = g(c, x_1),$$

$$y_{i+1} = g(y_i, x_{i+1}),$$

or

wherein the transformation section performs the predetermined transformation by the following recursion formulae for an integer i $(1 \le i \le m-1)$ and a predetermined integer c:

$$y_1 = g(c, x_1),$$

$$y_{i+1} = g(x_i, x_{i+1}).$$

28. (Canceled).

29. (New) The computer readable medium according to claim 27, wherein said mapping $h(\cdot)$ is defined by an operation of inverting a predetermined bit in a numerical expression of a given value instead of the operation of setting 01 to the least significant two bits.